JP2000330873 A

CONTENTS DISTRIBUTION SYSTEM, METHOD THEREFOR AND RECORDING MEDIUM

M KEN:KK

Inventor(s):SUZUKI AKIRA ;OGOSHI YUTAKA

Application No. 11136940 JP11136940 JP, Filed 19990518,A1 Published 20001130Published 20001130

Abstract:

PROBLEM TO BE SOLVED: To provide the structure of the whole system for protecting the copyright of digital contents distributed through a network by using digital watermark.

SOLUTION: The contents distribution system is provided with an application permission DB 12 for managing the identification(ID) information of contents permitted to appear on web pages, a contents retrieving part 14 for successively acquiring contents existing in respective web pages and an illegality detection part 16 for detecting illegal use by collating ID information as digital watermark extracted from acquired contents with ID information managed by the DB 12 and constituted so as to surely detect the illegal use of contents not permitted to appear on web pages by successively entering contents from respective web pages and detecting illegal use by judgment whether contents ID information padded as digital watermark in these contents is registered as contents permitted to appear on web pages or, not.

Int'l Class: G06F01214; G06T00100 H04N001387

Patents Citing This One (3):

→ WO0246935A1	20020613 SITEROCK K. K. SITE MONITORING METHOD AND SITE MONITORING SYSTEM
→ WO2003012651A1	20030213 ALPHABRIDGE CORPORATION CONTENT PROVIDING SYSTEM, CONTENT PROVIDING METHOD, CONTENT PROVIDING PROGRAM, AND COMPUTER-READABLE RECORDING MEDIUM
→ WO2003017109A1	20030227 ALPHABRIDGE CORPORATION

コンテンツ流通システムおよびその方法、記録媒体

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－330873
（P2000－330873A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
Ｇ０６Ｔ　1/00		Ｈ０４Ｎ　1/387		５Ｂ０５７
Ｈ０４Ｎ　1/387		Ｇ０６Ｆ　15/66	Ｂ	５Ｃ０７６

審査請求　未請求　請求項の数25　ＯＬ　（全 18 頁）

(21)出願番号　特願平11－136940

(22)出願日　平成11年５月18日(1999.5.18)

(71)出願人　597108822
株式会社エム研
東京都渋谷区元代々木町31番１号
(72)発明者　鈴木　晶
東京都渋谷区西原１－36－１
(72)発明者　大越　豊
東京都東久留米市学園町１－６－19
(74)代理人　100105784
弁理士　橘　和之

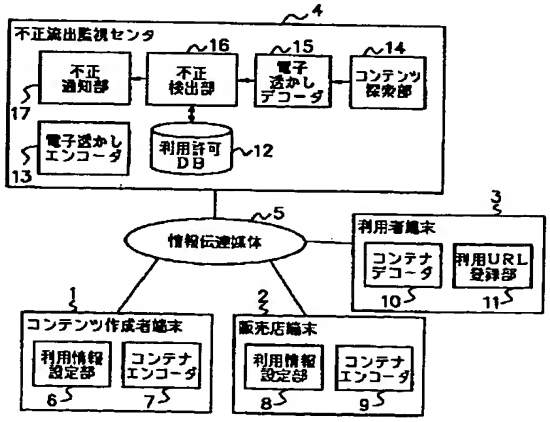
Ｆターム(参考)　5B017 AA06 AA07 BA05 BA07 BB02
BB10 CA08 CA09 CA16
5B057 CA12 CA16 CB12 CB16 CC01
CE08
5C076 AA14

(54)【発明の名称】　コンテンツ流通システムおよびその方法、記録媒体

(57)【要約】

【課題】　ネットワーク上で流通するデジタルコンテンツの著作権保護を電子透かしを用いて図るシステム全体の仕組みを提供する。

【解決手段】　ウェブページへの掲載が許可されたコンテンツの識別情報を管理する利用許可ＤＢ１２と、各ウェブページ上に存在するコンテンツを順次取得するコンテンツ探索部１４と、取得したコンテンツ中から取り出した電子透かしとしての識別情報と、利用許可ＤＢ１２により管理されている識別情報とを照合して不正利用を検出する不正検出部１６とを設け、ウェブページ上のコンテンツを順次取り込み、それらのコンテンツに電子透かしとして埋め込まれたコンテンツ識別情報が、ウェブページへの掲載を許可するものとして登録されているか否かによって不正利用を検出することにより、ウェブページへの掲載が許可されていないコンテンツの不正利用を確実に発見できるようにする。



【特許請求の範囲】

【請求項１】　デジタルコンテンツにその識別情報を電子透かしとして埋め込む電子透かし埋め込み手段と、
上記デジタルコンテンツのウェブページへの掲載の許否に関する情報を管理する許否情報管理手段と、
上記ウェブページを探索し、当該ウェブページ上に存在するデジタルコンテンツを取得するコンテンツ探索手段と、
上記取得したデジタルコンテンツの中から電子透かしとして埋め込まれた上記識別情報を取り出す電子透かし抽出手段と、
上記デジタルコンテンツの中から取り出された識別情報と、上記許否情報管理手段にて管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出する不正検出手段とを備えたことを特徴とするコンテンツ流通システム。

【請求項２】　上記許否情報管理手段は、上記ウェブページへの掲載が許可もしくは拒否されたデジタルコンテンツの識別情報を少なくとも管理し、
上記不正検出手段は、上記デジタルコンテンツの中から取り出された識別情報と、上記許否情報管理手段により管理されている識別情報とを照合して上記デジタルコンテンツの不正利用を検出することを特徴とする請求項１に記載のコンテンツ流通システム。

【請求項３】　上記許否情報管理手段は、上記ウェブページへの掲載が許可もしくは拒否されたデジタルコンテンツの識別情報と、上記デジタルコンテンツの掲載が許可もしくは拒否されたウェブページを表すリソース情報とを互いに対応付けて管理し、
上記不正検出手段は、上記デジタルコンテンツの中から取り出された識別情報および探索先のウェブページを表すリソース情報と、上記許否情報管理手段により管理されている識別情報およびリソース情報とを照合して上記デジタルコンテンツの不正利用を検出することを特徴とする請求項１に記載のコンテンツ流通システム。

【請求項４】　上記不正検出手段による検出結果を通知する不正通知手段を備えたことを特徴とする請求項１～３の何れか１項に記載のコンテンツ流通システム。

【請求項５】　上記不正通知手段は、上記不正検出手段による検出結果をＨＴＭＬファイル形式で記録し、そのＨＴＭＬファイルをウェブページに公開することを特徴とする請求項４に記載のコンテンツ流通システム。

【請求項６】　上記ＨＴＭＬファイルは、上記デジタルコンテンツの不正利用の検出先であるウェブページを表すリソース情報を含むことを特徴とする請求項５に記載のコンテンツ流通システム。

【請求項７】　上記コンテンツ探索手段は、ウェブサイトに移動してそこのウェブページ上に存在するコンテンツファイルを順次ダウンロードするソフトウェアモジュールにより構成されることを特徴とする請求項１～３の何れか１項に記載のコンテンツ流通システム。

【請求項８】　上記コンテンツ探索手段は、上記ウェブサイトに張られたリンクを辿ることによってネットワーク上のウェブページを順次探索することを特徴とする請求項７に記載のコンテンツ流通システム。

【請求項９】　上記ウェブサイトに張られたリンクを辿る際に、探索済のウェブページを表す情報を履歴として保持しておき、この履歴を参照することによって一度探索したウェブページは探索しないようにすることを特徴とする請求項８に記載のコンテンツ流通システム。

【請求項１０】　上記コンテンツ探索手段は、上記デジタルコンテンツを多く持つウェブサイトに張られたリンクを重視してネットワーク上のウェブページを順次探索することを特徴とする請求項８に記載のコンテンツ流通システム。

【請求項１１】　暗号化されたデジタルコンテンツを配付する配付手段と、上記デジタルコンテンツの提供を受けて利用する利用手段と、上記デジタルコンテンツの利用料をユーザに対して課金し、上記利用料の支払いを条件に各デジタルコンテンツ毎に固有の暗号鍵を発行する課金・利用許可発行手段とを有し、入手したデジタルコンテンツの利用に対して課金を行うようになされたコンテンツ流通システムであって、
上記課金・利用許可発行手段は、上記各デジタルコンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵を発行し、上記暗号鍵とユーザ鍵の両方を用いて上記デジタルコンテンツの利用を制限するようにしたことを特徴とするコンテンツ流通システム。

【請求項１２】　上記暗号鍵をユーザが取得する際に、上記暗号鍵の発行元において、上記暗号鍵の利用を上記ユーザ鍵で制限する処理を行うことを特徴とする請求項１１に記載のコンテンツ流通システム。

【請求項１３】　上記暗号鍵に基づき暗号化されたデジタルコンテンツをユーザが取得する際に、上記デジタルコンテンツの配付元において、上記暗号化されたデジタルコンテンツの利用を上記ユーザ鍵で制限する処理を行うことを特徴とする請求項１１に記載のコンテンツ流通システム。

【請求項１４】　上記暗号鍵に基づき暗号化されたデジタルコンテンツをユーザが取得した際に、上記デジタルコンテンツの取得先において、上記暗号化されたデジタルコンテンツの利用を上記ユーザ鍵で制限する処理を行うことを特徴とする請求項１１に記載のコンテンツ流通システム。

【請求項１５】　上記暗号鍵をユーザが取得した際に、上記暗号鍵の取得先において、上記暗号鍵の利用を上記ユーザ鍵で制限する処理を行うことを特徴とする請求項１１に記載のコンテンツ流通システム。

【請求項１６】　入手したデジタルコンテンツの利用に

対して課金を行うコンテンツ流通システムであって、
上記デジタルコンテンツのウェブページへの張り付けを含む各種用途のうち利用を許可もしくは拒否する用途を設定する利用情報設定手段と、
上記デジタルコンテンツのウェブページへの掲載の許否に関する情報を管理する許否情報管理手段と、
上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限する利用制限手段と、
上記デジタルコンテンツにその識別情報を電子透かしとして埋め込む電子透かし埋め込み手段と、
上記ウェブページを探索し、当該ウェブページ上に存在するデジタルコンテンツを取得するコンテンツ探索手段と、
上記取得したデジタルコンテンツ中から電子透かしとして埋め込まれた上記識別情報を取り出す電子透かし抽出手段と、
上記デジタルコンテンツ中から取り出された識別情報と、上記許否情報管理手段により管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出する不正検出手段とを備えたことを特徴とするコンテンツ流通システム。

【請求項１７】　上記許否情報管理手段は、上記ウェブページへの掲載が許可もしくは拒否されたデジタルコンテンツの識別情報を少なくとも管理し、
上記不正検出手段は、上記デジタルコンテンツの中から取り出された識別情報と、上記許否情報管理手段により管理されている識別情報とを照合して上記デジタルコンテンツの不正利用を検出することを特徴とする請求項１６に記載のコンテンツ流通システム。

【請求項１８】　上記許否情報管理手段は、上記ウェブページへの掲載が許可もしくは拒否されたデジタルコンテンツの識別情報と、上記デジタルコンテンツの掲載が許可もしくは拒否されたウェブページを表すリソース情報とを互いに対応付けて管理し、
上記不正検出手段は、上記デジタルコンテンツの中から取り出された識別情報および探索先のウェブページを表すリソース情報と、上記許否情報管理手段により管理されている識別情報およびリソース情報とを照合して上記デジタルコンテンツの不正利用を検出することを特徴とする請求項１６に記載のコンテンツ流通システム。

【請求項１９】　上記不正検出手段による検出結果を通知する不正通知手段を備えたことを特徴とする請求項１６～１８の何れか１項に記載のコンテンツ流通システム。

【請求項２０】　ネットワーク上に存在するウェブページへのデジタルコンテンツの掲載の許否に関する情報を管理するようになし、
上記ウェブページを探索して当該ウェブページ上にあるデジタルコンテンツを取得し、取得したデジタルコンテンツの中から電子透かしとして埋め込まれている上記デジタルコンテンツの識別情報を取り出し、当該取り出した識別情報と上記管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出するようにしたことを特徴とするコンテンツ流通方法。

【請求項２１】　入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムにおいて、上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限するようにしたことを特徴とするコンテンツ流通方法。

【請求項２２】　入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムにおいて、上記デジタルコンテンツのウェブページへの張り付けを含む各種用途のうち利用を許可もしくは拒否する用途を設定し、上記デジタルコンテンツのウェブページへの掲載の許否に関する情報を管理するようになし、
上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限するようにするとともに、
上記ウェブページを探索して当該ウェブページ上にあるデジタルコンテンツを取得し、取得したデジタルコンテンツの中から電子透かしとして埋め込まれている上記デジタルコンテンツの識別情報を取り出し、当該取り出した識別情報と上記管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出するようにしたことを特徴とするコンテンツ流通方法。

【請求項２３】　請求項１～４、１６～１９の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２４】　入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムにおいて、上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限する利用制限手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２５】　請求項２０～２２の何れか１項に記載のコンテンツ流通方法の処理手順をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ流通システムおよびその方法、更にはこれらを実現するプログ

ラムを格納した記録媒体に関するものであり、特に、オープンな広域ネットワーク上で流通する画像データや音声データ等のデジタルコンテンツの著作権を保護するための仕組みに関するものである。

【０００２】

【従来の技術】近年、情報通信関連の技術革新に伴って、インターネット等のオープンなコンピュータネットワークを用いて大容量のデジタルデータをやり取りすることが簡単にできるようになってきた。このインターネット上では、応用プログラムや音楽、画像、ゲーム等のデジタル著作物（デジタルコンテンツ）のやり取りも盛んに行われている。

【０００３】これらのデジタルコンテンツは、複製・編集・伝送などの操作が容易であり、またこれらの操作を行っても品質の劣化が起こらないという特徴を持つ。そのため、正当な権利を持たない第三者がデジタルコンテンツを不正に利用することが予想される。そこで、コンテンツ提供者の権利を保護するという観点から、デジタルコンテンツに対する課金方式や不正コピー等の防止もしくは摘発技術の実現が不可欠となっている。

【０００４】従来、デジタルコンテンツの著作権を保護するために、デジタルデータ中に電子透かしを埋め込んで管理するシステムが提案されている。電子透かしとは、デジタルコンテンツやその著作者を識別するための権利情報などを改ざん困難な形でデジタルコンテンツ内に埋め込む技術である。この電子透かしを用いたシステムでは、コンテンツ提供者等の著作者は、デジタルコンテンツと権利情報とをサービス事業者に預託し、このサービス事業者が持つ埋め込みサーバ等により電子透かし入りコンテンツの作成を行っていた。

【０００５】また、近年においては、デジタルコンテンツに対する課金方式として、超流通システムなる技術が提案されてきている。超流通とは、複製が簡単であるデジタルデータの特性を活かして、デジタルコンテンツのコピー自体は許してその利用に対して課金を行おうとするものである。すなわち、これは、デジタルコンテンツを暗号化しておき、その暗号化されたデジタルコンテンツを入手することは自由にできるが、暗号を解くための暗号鍵を利用者が購入しない限り利用できないようにすることによって著作権保護を図ろうとするものである。

【０００６】

【発明が解決しようとする課題】しかしながら、上記電子透かしは近年になって着目されてきた技術であり、その埋め込み方式や埋め込みシステム、あるいは埋め込んだ電子透かしの抽出方式等の技術については種々のアイデアが提案されているものの、デジタルコンテンツ中に埋め込んだ電子透かしを用いて不正利用をどのように摘発するかといったシステム全体の仕組みについては何ら考えられていなかった。

【０００７】また、暗号化技術を利用した超流通システムでは、デジタルコンテンツを利用するに当たって利用者に課せられている条件は、暗号鍵に対する課金だけであり、課金を行った後の不正利用を防止する手段については何ら講じられていなかった。そのため、デジタルコンテンツの利用に何ら制限を設けないと、利用者が暗号鍵を購入して暗号を復号した後は複製や編集等が全く自由に行えるようになるため、例えば再販を行うなどの不正利用に供されることもある。そのため、従来の超流通システムでは、暗号鍵を購入した場合でもデジタルコンテンツの利用に制限を設けざるを得ず、ユーザの要求に応じた様々な態様でデジタルコンテンツを提供することはできなかった。

【０００８】さらに、購入した暗号鍵を第三者に配付すれば、デジタルコンテンツ自体は無料で入手できるため、第三者はその暗号鍵を用いてデジタルコンテンツを利用することが可能となってしまう。つまり、従来の超流通システムでは、１次的な利用者に対して課金という条件を課すことができるのみで、著作権の厳密な保護は図れていなかった。

【０００９】本発明は、このような実情に鑑みて成されたものであり、ネットワーク上で流通するデジタルコンテンツの著作権保護を図るための電子透かしを用いたシステム全体の仕組みを提供することを目的とする。また、本発明は、超流通システムにおいてデジタルコンテンツの不正利用をより確実に防止できるようにすることをも目的とする。さらに、本発明は、超流通システムにおけるデジタルコンテンツの利用制限を緩和して様々な態様でデジタルコンテンツを利用できるようにするとともに、その不正利用を確実に摘発できるようにすることをも目的とする。

【００１０】

【課題を解決するための手段】本発明のコンテンツ流通システムは、デジタルコンテンツにその識別情報を電子透かしとして埋め込む電子透かし埋め込み手段と、上記デジタルコンテンツのウェブページへの掲載の許否に関する情報を管理する許否情報管理手段と、上記ウェブページを探索し、当該ウェブページ上に存在するデジタルコンテンツを取得するコンテンツ探索手段と、上記取得したデジタルコンテンツの中から電子透かしとして埋め込まれた上記識別情報を取り出す電子透かし抽出手段と、上記デジタルコンテンツの中から取り出された識別情報と、上記許否情報管理手段にて管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出する不正検出手段とを備えたことを特徴とする。

【００１１】例えば、上記許否情報管理手段は、上記ウェブページへの掲載が許可もしくは拒否されたデジタルコンテンツの識別情報を少なくとも管理し、上記不正検出手段は、上記デジタルコンテンツの中から取り出された識別情報と、上記許否情報管理手段により管理されている識別情報とを照合して上記デジタルコンテンツの不

正利用を検出する。また、上記許否情報管理手段は、上記ウェブページへの掲載が許可もしくは拒否されたデジタルコンテンツの識別情報と、上記デジタルコンテンツの掲載が許可もしくは拒否されたウェブページを表すリソース情報とを互いに対応付けて管理し、上記不正検出手段は、上記デジタルコンテンツの中から取り出された識別情報および探索先のウェブページを表すリソース情報と、上記許否情報管理手段により管理されている識別情報およびリソース情報とを照合して上記デジタルコンテンツの不正利用を検出するようにしても良い。

【００１２】本発明の他の態様では、上記不正検出手段による検出結果を通知する不正通知手段を備えたことを特徴とする。ここで、上記不正通知手段は、上記不正検出手段による検出結果をＨＴＭＬファイル形式で記録し、そのＨＴＭＬファイルをウェブページに公開するようにしても良い。また、上記ＨＴＭＬファイルは、上記デジタルコンテンツの不正利用の検出先であるウェブページを表すリソース情報を含むものであっても良い。

【００１３】本発明のその他の態様では、暗号化されたデジタルコンテンツを配付する配付手段と、上記デジタルコンテンツの提供を受けて利用する利用手段と、上記デジタルコンテンツの利用料をユーザに対して課金し、上記利用料の支払いを条件に各デジタルコンテンツ毎に固有の暗号鍵を発行する課金・利用許可発行手段とを有し、入手したデジタルコンテンツの利用に対して課金を行うようになされたコンテンツ流通システムであって、上記課金・利用許可発行手段は、上記各デジタルコンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵を発行し、上記暗号鍵とユーザ鍵の両方を用いて上記デジタルコンテンツの利用を制限するようにしたことを特徴とする。

【００１４】本発明のその他の態様では、入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムであって、上記デジタルコンテンツのウェブページへの張り付けを含む各種用途のうち利用を許可もしくは拒否する用途を設定する利用情報設定手段と、上記デジタルコンテンツのウェブページへの掲載の許否に関する情報を管理する許否情報管理手段と、上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限する利用制限手段と、上記デジタルコンテンツにその識別情報を電子透かしとして埋め込む電子透かし埋め込み手段と、上記ウェブページを探索し、当該ウェブページ上に存在するデジタルコンテンツを取得するコンテンツ探索手段と、上記取得したデジタルコンテンツ中から電子透かしとして埋め込まれた上記識別情報を取り出す電子透かし抽出手段と、上記デジタルコンテンツ中から取り出された識別情報と、上記許否情報管理手段により管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出する不正検出手段とを備える。

【００１５】また、本発明のコンテンツ流通方法は、ネットワーク上に存在するウェブページへのデジタルコンテンツの掲載の許否に関する情報を管理するようになし、上記ウェブページを探索して当該ウェブページ上にあるデジタルコンテンツを取得し、取得したデジタルコンテンツの中から電子透かしとして埋め込まれている上記デジタルコンテンツの識別情報を取り出し、当該取り出した識別情報と上記管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出するようにしたことを特徴とする。

【００１６】本発明の他の態様では、入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムにおいて、上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限するようにしたことを特徴とする。

【００１７】本発明のその他の態様では、入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムにおいて、上記デジタルコンテンツのウェブページへの張り付けを含む各種用途のうち利用を許可もしくは拒否する用途を設定し、上記デジタルコンテンツのウェブページへの掲載の許否に関する情報を管理するようになし、上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限するようにするとともに、上記ウェブページを探索して当該ウェブページ上にあるデジタルコンテンツを取得し、取得したデジタルコンテンツの中から電子透かしとして埋め込まれている上記デジタルコンテンツの識別情報を取り出し、当該取り出した識別情報と上記管理されている情報とを照合して上記デジタルコンテンツの不正利用を検出するようにしたことを特徴とする。

【００１８】また、本発明のコンピュータ読み取り可能な記録媒体は、請求項１～４、１６～１９の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とする。本発明の他の態様では、入手したデジタルコンテンツの利用に対して課金を行うコンテンツ流通システムにおいて、上記デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、上記デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いて上記デジタルコンテンツの利用を制限する利用制限手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とする。本発明のその他の態様では、請求項２０～２２の何れか１項に記載のコンテンツ流通方法の処理手順をコンピュータに実行させるためのプログラムを記録したこと

を特徴とする。

【００１９】本発明は上記技術手段より成るので、ネットワークのウェブページ上にあるデジタルコンテンツが順次取り込まれ、それらのデジタルコンテンツに電子透かしとして埋め込まれたコンテンツ識別情報と、ウェブページへの掲載を許可もしくは拒否するものとして管理されている情報とを照合することによって、ウェブページへの掲載が許可されていないデジタルコンテンツの不正利用等を発見することが可能となる。

【００２０】また、デジタルコンテンツの掲載が許可されたウェブページを表すリソース情報をコンテンツ識別情報と対応付けて管理し、このリソース情報も加味して不正検出を行うようにした本発明によれば、ウェブページへの掲載自体は許可されているが、許可されていないウェブページに掲載されたデジタルコンテンツの不正利用等を発見することが可能となる。

【００２１】また、暗号鍵の他にユーザ鍵も用いてデジタルコンテンツの利用を制限するようにした本発明によれば、デジタルコンテンツを正当に購入していない第三者に対してデジタルコンテンツとその暗号鍵を配付したとしても、その第三者はユーザ鍵を持たないためにデジタルコンテンツを利用することができず、正当に購入したユーザだけにデジタルコンテンツの利用を制限することが可能となる。

【００２２】また、上述の電子透かしに関する発明とユーザ鍵に関する発明とを組み合わせて適用した本発明によれば、正当に購入したユーザだけにデジタルコンテンツの利用を制限することが可能となるだけでなく、正当にデジタルコンテンツを購入したユーザがその後、許可されていないにも関わらずウェブページへの掲載を行ったり、許可されていないウェブページへの掲載を行ったりしたことも発見することが可能となる。

【００２３】

【発明の実施の形態】（第１の実施形態）図１は、本発明の第１の実施形態によるコンテンツ流通システムの全体構成を示すブロック図である。

【００２４】図１において、１はデジタルコンテンツ（以下、コンテンツと略す）の作成者やプロダクション等が使用するコンテンツ作成者端末、２はコンテンツを配付する販売店等が使用する販売店端末、３はコンテンツの提供を受けて利用するユーザ等が使用する利用者端末、４はコンテンツの不正流出を監視する不正流出監視センタ、５はインターネット等のネットワーク、あるいはＣＤ－ＲＯＭやフロッピーディスク等の記録メディアにより構成される情報伝達媒体である。

【００２５】本実施形態のコンテンツ流通システムは、上記コンテンツ作成者端末１、販売店端末２、利用者端末３および不正流出監視センタ４が、インターネットやＣＤ－ＲＯＭ等の情報伝達媒体５を介して以下に述べるような種々の情報をやり取りすることができるように構成されている。なお、ここでは図面の都合上、コンテンツ作成者端末１、販売店端末２、利用者端末３を１つずつ示しているが、それぞれ複数存在しても良い。

【００２６】上記コンテンツ作成者端末１は、利用情報設定部６とコンテナエンコーダ７とを備える。利用情報設定部６は、コンテンツ作成者やプロダクション等の著作者がコンテンツを提供する際に、提供を受けるユーザが利用可能な範囲を表す情報を設定する。この利用可能情報は、例えば利用有効期限、利用回数、通算使用時間などの制限情報、著作権料などの価格情報、コンテンツを利用する際の用途を規制する用途情報などを含む。用途情報としては少なくとも、コンテンツの表示あるいは再生のみ、およびウェブページ（ウェブサイト）への張り付け許可を含む。上述の著作権料は、これらの用途ごとに設定することが可能である。

【００２７】また、コンテナエンコーダ７は、作成されたコンテンツと、そのコンテンツの利用に必要な上記利用可能情報とを１つのファイルにまとめる処理を行う。このようにコンテンツと利用可能情報とが１つのファイルにまとめられたものを「コンテナ」と呼ぶ。情報伝達媒体５上でコンテンツは、そのままの形態ではなく、このコンテナの形で流通する。なお、ここでは図示していないが、暗号鍵を用いてコンテンツを暗号化し、暗号化したコンテンツと利用可能情報とをまとめてコンテナ化するようにしても良い。

【００２８】また、上記販売店端末２も、利用情報設定部８とコンテナエンコーダ９とを備える。販売店は、コンテンツ作成者端末１にて作成されたコンテナの提供を受けて、例えばウェブページ上にユーザがダウンロードできる形で陳列する。また、ＣＤ－ＲＯＭ等の記録メディアを利用してオフラインでコンテナを配付することも可能である。販売店は、配付するコンテナの宣伝等も行う。

【００２９】販売店端末２の利用情報設定部８は、上述のような販売のための各種サービス等に対する手数料を設定する。また、コンテナエンコーダ９は、コンテンツ作成者端末１にて作成されたコンテナと上記手数料等の価格情報とを１つのファイルにまとめ、更にコンテナ化する。なお、ここでは著作権者と販売店が異なる場合を例に挙げているが、著作者自身がコンテナの販売を行っても良く、その場合にはこの販売店端末２は不要である。

【００３０】また、利用者端末３は、コンテナデコーダ１０と利用ＵＲＬ登録部１１とを備える。コンテナデコーダ１０は、コンテンツ作成者や販売店から配付を受けたコンテナに対して所定の処理を行うことにより、利用可能情報や販売手数料などの情報が付加されたコンテナ内のコンテンツを利用できる形態に変換する。その際にユーザは、コンテナ内に含まれている利用可能情報を参照して、どの用途でコンテンツを利用するかを決定す

る。

【００３１】例えば、コンテンツに暗号化が施されている場合は、コンテナデコーダ１０でその復号処理を行う。この復号処理を行うためには暗号鍵が必要であるため、ユーザはその暗号鍵を購入することになる。この場合、コンテナ自体の入手は無料としても良い。なお、コンテンツに暗号化処理が施されていない場合には、用途に応じた料金の支払いを条件にコンテナの配付を行うようにしても良い。

【００３２】また、利用ＵＲＬ登録部１１は、ユーザがコンテンツをウェブページに張り付けて使用することを選択した場合に、どのコンテンツをどのウェブページ上に張り付けるかの情報（例えば、ウェブページに張り付けるコンテンツの識別情報とウェブページのリソース場所であるＵＲＬ（Uniform Resource Locator）情報）を不正流出監視センタ４に登録する。これらの情報は、不正流出監視センタ４内で利用許可データベース（ＤＢ）１２として保存、管理される。

【００３３】なお、上記コンテンツ作成者端末１内の利用情報設定部６で設定された利用可能情報も、この利用許可ＤＢ１２に登録され、保存、管理される。すなわち、不正流出監視センタ４は、利用可能情報としてウェブページへの張り付け許可が記述されたコンテンツの識別情報、つまり、どのコンテンツがユーザのウェブページに張り出しても良いのかを表すコンテンツＩＤをコンテンツ作成者端末１から受け取り、それを利用許可ＤＢ１２に格納する。

【００３４】また、上記不正流出監視センタ４は、上述の利用許可ＤＢ１２の他に、電子透かしエンコーダ１３、コンテンツ探索部１４、電子透かしデコーダ１５、不正検出部１６および不正通知部１７を備える。上記電子透かしエンコーダ１３は、コンテンツ作成者により作成されたコンテンツを受け取り、電子透かしを埋め込んで返却する処理を行う。したがって、上述のようにコンテンツ作成者端末１、販売店端末２および利用者端末３間で流通するコンテナ内のコンテンツは、電子透かしが埋め込まれたものである。ここで埋め込む電子透かしは、例えばそのコンテンツを識別するためのユニークなコンテンツＩＤである。

【００３５】コンテンツ探索部１４は、インターネット上を巡回し、ウェブページに置かれたコンテンツファイルを自動的にダウンロードする。すなわち、ウェブページ上に掲載されている様々な形態のデータファイルのうち、画像ファイルや音楽ファイル等の著作権に関連するコンテンツファイルを探し出してダウンロードする。これらのコンテンツファイルは、例えばファイル名の拡張子を見ることによって識別することが可能である。

【００３６】このコンテンツ探索部１４は、例えば、何を処理するべきかを自ら判断して実行できるソフトウェアモジュール（エージェント）により構成される。つまり、コンテンツ探索部１４のエージェントは、インターネット上に存在するウェブサイトに常駐してそこに置かれたコンテンツファイルを自動的にダウンロードし、１つのウェブサイトでの処理が終わったら次のウェブサイトに移動して、そこのコンテンツファイルをダウンロードするという処理を順次行っていく。

【００３７】このとき、ウェブサイト間の移動は、各ウェブサイトに張られたリンクを利用して行う。すなわち、最初は初期登録されたウェブサイトに移動してそこのウェブページに置かれているコンテンツファイルのダウンロードを行い、その後は各ウェブサイトに張られたリンクを辿ることによってインターネット上のウェブページを順次探索する。このとき、どのウェブページを探索したかをＵＲＬの履歴として保持しておき、一度探索したウェブページは再び探索しないようにすることができる。

【００３８】このようにリンクを辿ってインターネット上のウェブサイトを順次探索していき、或るウェブサイトから張られた次のリンク先のＵＲＬが全て履歴の中に存在することとなった場合には、インターネット上に存在するウェブページの探索が一巡したことになる。この場合は、再び初期登録されたウェブサイトに戻り、以下同様にしてコンテンツファイルのダウンロードを自動実行する。

【００３９】なお、インターネット上に存在するウェブページの数は非常に多いため、全てのウェブページを巡回するには多くの時間がかかる。そこで、このダウンロードの処理を高速化するために、コンテンツ探索部１４のエージェントを複数設け、巡回を並列処理で行うようにしても良い。

【００４０】また、リンクを辿る際に、コンテンツファイルを多く有するウェブサイトが運営するリンクを重視して巡回を行うようにすることも可能である。これは、画像や音楽等のコンテンツファイルを多く有するウェブサイトには、同じくコンテンツファイルを多く有する同業者等のウェブサイトがリンクしていることが多いためである。

【００４１】例えば、インターネット上のウェブサイトを最初に巡回する際に、各ウェブサイトの中にあるコンテンツファイルの数をファイル拡張子をもとに数えることにより、コンテンツファイルを多く有するウェブサイトを把握する。そして、２巡目以降ではコンテンツファイルを多く有するウェブサイトを優先してリンクを辿るようにする。このようにすれば、インターネット上に存在する数多くのウェブページを効率的に探索することができる。

【００４２】また、上記電子透かしデコーダ１５は、コンテンツ探索部１４がダウンロードしてきたコンテンツファイルの中から電子透かしとして埋め込まれたコンテンツＩＤを取り出す。コンテンツ探索部１４がコンテン

ツファイルをダウンロードしてくる速度に対して電子透かしデコーダ１５の処理速度が十分でなく、処理の渋滞を起こす可能性がある場合には、この電子透かしデコーダ１５を複数設け、電子透かしのデコードを並列処理で行うようにしても良い。

【００４３】不正検出部１６は、電子透かしデコーダ１５によりコンテンツ内から取り出された電子透かしとしてのコンテンツＩＤと、利用許可ＤＢ１２に登録されているコンテンツＩＤとを照合して、ダウンロードされてきたコンテンツがウェブページへの掲載が許可されたコンテンツであるかどうかを検査する。ここで、コンテンツ内から取り出されたコンテンツＩＤが利用許可ＤＢ１２に登録されていない場合には、そのコンテンツは不正に利用されたものであるということを検出することができる。

【００４４】このとき、不正検出部１６においてコンテンツの不正利用を検出する際に、コンテンツ作成者端末１から利用許可ＤＢ１２に登録されたコンテンツＩＤを用いれば、ウェブページへの張り付け自体が許可されていないコンテンツがユーザによって不正に張り付けられたことを少なくとも検出することができる。これにより、ユーザに提供された画像や音楽等のコンテンツがウェブページ上で販売されるなどの不正利用を発見することができる。

【００４５】さらに、利用ＵＲＬ登録部１１から利用許可ＤＢ１２に登録されたＵＲＬ情報も用いれば、ダウンロードされたコンテンツ内から取り出したコンテンツＩＤとダウンロード先のＵＲＬとを利用許可ＤＢ１２に問い合わせることにより、ウェブページへの張り付け自体は許可されているが、許可されていないＵＲＬのウェブページにそのコンテンツが不正に張り付けられたことをも検出することができる。これにより、或るユーザに提供されたコンテンツが無断で第三者に配付され、その第三者のウェブページ上にて無断で販売が行われるなどの不正利用を発見することができる。

【００４６】不正通知部１７は、不正検出部１６によってコンテンツの不正流出が検出された場合に、その旨をコンテンツ作成者等の著作者に通知する。この通知は、例えばメールによって行うことが可能である。また、不正検出部１６による検査結果をＨＴＭＬ（Hyper Text Markup Language）ファイル形式で記録し、その記録ファイルを不正流出監視センタ４のウェブサイトに公開することによって行うようにしても良い。このようにすれば、検査結果の確認をしたい著作者等が、コンテンツの不正利用状況を手元のウェブブラウザを用いていつでも簡単に確認することができる。

【００４７】また、検査結果をウェブサイトに公開する際に、検査結果のＨＴＭＬファイルに不正利用検出先のＵＲＬを記載するようにしても良い。このようにすることにより、検査結果の確認者が、手元のウェブブラウザを用いて検査対象のコンテンツファイルがあるウェブサイトに容易にアクセスすることができ、そこに置かれているコンテンツの確認等を容易に行うことができるようになる。

【００４８】図２は、上記図１のように構成したコンテンツ流通システムにおいて行われる一連の動作を説明するための図である。図２において、まず最初にコンテンツ作成者やプロダクション等の著作者は、コンテンツ作成者端末１においてコンテンツを作成し、その作成したコンテンツを不正流出監視センタ４に預ける。不正流出監視センタ４は、電子透かしエンコーダ１３を用いて、預かったコンテンツ内にコンテンツＩＤを電子透かしとして埋め込み、それをコンテンツ作成者端末１に返す。

【００４９】また、著作者は、コンテンツの利用可能範囲や著作権料を決めて、利用可能情報を設定する。このとき、コンテンツ作成者端末１内のコンテナエンコーダ７によって、利用可能情報でウェブページへの掲載が許可されたコンテンツのＩＤが不正流出監視センタ４に通知され、利用許可ＤＢ１２に登録される。さらに著作者は、コンテナエンコーダ７を用いて、電子透かしの埋め込まれたコンテンツと利用可能情報とをコンテナ化する。そして、このようにして作成したコンテナファイルを販売店に納める。

【００５０】販売店は、自らの販売手数料を上乗せしてコンテナの販売価格（利用料）を設定し、コンテナエンコーダ９を用いてコンテナファイル内の利用可能情報に追加する。そして、このようにして２次的にコンテナ化したファイルを販売店のウェブサイトに掲載したり、ＣＤ－ＲＯＭに納めることなどによってコンテナの販売を行う。なお、上述したように、著作者自身が販売店となってコンテナを販売することも可能である。

【００５１】ユーザは、販売店のウェブサイトからコンテナをダウンロードしたり、ＣＤ－ＲＯＭを介してコンテナを入手する。そして、入手したコンテナ内の利用可能情報を参照して利用可能な用途と利用価格を把握し、利用したい用途を選択する。このとき、コンテンツをウェブページに張り付けて利用することを選択した場合は、そのウェブページのＵＲＬとコンテンツＩＤとが利用ＵＲＬ登録部１１によって不正流出監視センタ４に通知され、利用許可ＤＢ１２に登録される。

【００５２】ユーザは、選択した用途に応じた利用料を販売店もしくは著作者に支払う。これは、インターネットのオンライン上で電子マネーを利用して行っても良いし、オフラインで行っても良い。この利用料を支払うことによって始めてコンテナデコーダ１０が利用できるようになり（例えば、コンテンツが暗号化されている場合には暗号鍵が与えられる）、ユーザは、この利用可能となったコンテナデコーダ１０を用いて、コンテナ内のコンテンツを利用できる形態に変換する。

【００５３】本実施形態において、コンテンツの利用形

態としては、再生のみを可能とする再生利用と、ウェブページへの張り付けを可能とする抜き出し利用との２パターンがある。再生利用の場合、コンテナデコーダ１０は、内部メモリ上で展開したコンテンツファイルを静止画や動画であれば表示し、音楽であればスピーカに出力する。ただし、汎用の画像フォーマットや音楽フォーマットのファイルとして外部記憶装置に書き込むことはしない。よって、再生後にユーザの手元にコンテンツファイルが残ることはない。

【００５４】一方、抜き出し利用の場合、上記コンテナデコーダ１０は、内部メモリ上で展開したコンテンツファイルを汎用フォーマットのデータファイルに変換してコンテナデコーダ１０の外部に出力し、外部記憶装置に書き込む。これによりユーザは、コンテンツをウェブページに張り付けて利用することを選択した場合には、コンテナ内からコンテンツを取り出してウェブページに張り付けることが可能となる。

【００５５】不正流出監視センタ４では、コンテンツ探索部１４（エージェントで構成される検索ロボット）を用いて、インターネット上のウェブサイトを巡回して各ウェブページに置かれたコンテンツを順次ダウンロードする。このとき、不正流出しているコンテンツがウェブページ上に置かれていれば、それもダウンロードされる。

【００５６】さらに、不正流出監視センタ４では、電子透かしデコーダ１５を用いて、ダウンロードしたコンテンツの中から電子透かしを取り出し、そのコンテンツに固有のＩＤを検出する。そして、不正検出部１６において、その検出したコンテンツＩＤおよびダウンロード先のＵＲＬと、利用許可ＤＢ１２に登録されているコンテンツＩＤおよびＵＲＬとを照合することにより、コンテンツの不正利用の検出を行う。

【００５７】すなわち、利用許可ＤＢ１２に登録されていないコンテンツＩＤを検出した場合や、ユーザが正規料金を支払ってコンテンツを張り付けたウェブページのＵＲＬ以外の場所でコンテンツＩＤを検出した場合には、そのコンテンツは無許可で張り付けられたものということになる。よって、この場合には、不正通知部１７を用いて、不正利用を摘発したコンテンツＩＤとそれが置かれていたウェブページのＵＲＬとをそのコンテンツの著作者に通知する。また、そのウェブページの運営者に警告を発するようにしても良い。

【００５８】以上説明したように、本実施形態では、インターネット上のウェブサイトを巡回してそこに置かれたウェブページ上のコンテンツファイルを順次ダウンロードし、それらのコンテンツに電子透かしとして埋め込まれているコンテンツＩＤが、利用を許可するものとして登録されているか否かを検出するようにしている。これにより、ウェブページへの張り付けが許可されていないコンテンツの不正利用や、許可されていないウェブページへの張り付け等の不正利用を常に監視し、コンテンツの不正利用を有効に発見することができる。

【００５９】なお、上記実施形態では、コンテンツファイルをコンテナ化する前に不正流出監視センタ４において電子透かしを埋め込む例を示しているが、電子透かしは、最終的にユーザが入手したコンテンツをウェブページに張り付けるまでの間に埋め込まれていれば良く、その埋め込む場所やタイミングは上記の例に限定されない。例えば、ユーザが利用者端末３上に入手したコンテナからコンテンツを取り出すときに電子透かしを埋め込むようにしても良い。

【００６０】また、上記実施形態では、コンテンツ作成者端末１と利用者端末３の両方から不正流出監視センタ４の利用許可ＤＢ１２にウェブページ張り付けの利用許可に関する情報を登録しているが、どちらか一方のみから登録を行うようにしても良い。また、ここでは利用許可に関する情報を登録しているが、利用拒否に関する情報を登録するようにしても良い。

【００６１】例えば、上記実施形態では著作者が作成したコンテンツを第三者に販売することを前提としているが、著作者以外の利用は全く許さないようにすることも考えられる。この場合には、作成したコンテンツのＩＤを利用拒否に関する情報として登録しておき、ダウンロードしたコンテンツ内から取り出したコンテンツＩＤがこの登録されたＩＤと一致するか否かを見ることによって、不正利用を検出するようにしても良い。なお、この場合には、コンテンツの価格情報や用途情報の設定等は不要である。

【００６２】また、上記実施形態では、コンテンツを利用可能情報と共に１つのファイルにまとめたコンテナとして流通する例を示したが、必ずしもコンテナ化する必要はない。例えば、コンテンツの流通と利用可能情報の流通とを別個に行うようにしても良い。

【００６３】（第２の実施形態）次に、本発明によるコンテンツ流通システムの第２の実施形態について説明する。以下に述べる第２の実施形態は、本発明を超流通システムに適用したものである。図３は、第２の実施形態によるコンテンツ流通システムの全体構成を示すブロック図である。なお、図３において、図１に示したブロックと同じブロックには同一の符号を付している。

【００６４】図３に示すように、第２の実施形態によるコンテンツ流通システムは、コンテンツ作成者端末１、販売店端末２、利用者端末３、ライセンス発行センタ２１および課金センタ２２が、インターネットやＣＤ－ＲＯＭ等の情報伝達媒体５を介して以下に述べるような種々の情報をやり取りすることができるように構成されている。なお、ここでは図面の都合上、コンテンツ作成者端末１、販売店端末２、利用者端末３を１つずつ示しているが、それぞれ複数存在しても良い。

【００６５】本実施形態のコンテンツ作成者端末１は、

利用情報設定部６とコンテナエンコーダ１９とを備える。コンテナエンコーダ１９は、コンテンツ作成者によって作成されたコンテンツと、そのコンテンツの利用に必要な上記利用可能情報とを１つのファイルにまとめる処理を行う。図４は、このコンテナエンコーダ１９の構成例を示す図である。

【００６６】図４において、３１はコンテナ鍵生成部であり、コンテンツファイルを暗号化するために必要な暗号鍵であるコンテナ鍵を生成する。このコンテナ鍵は、個々のコンテンツに固有の暗号鍵であり、利用者端末３内のコンテナデコーダ２０（この構成については後述する）においてコンテナ内の暗号化コンテンツファイルを復号する際の復号鍵でもある。

【００６７】３２はコンテナ鍵登録部であり、上記コンテナ鍵生成部３１により生成されたコンテナ鍵をライセンス発行センタ２１に登録する。ユーザは、このコンテナ鍵をライセンス発行センタ２１から購入することで、暗号化コンテンツを復号して利用することが可能となる。３３はコンテンツ入力部であり、コンテンツ作成者により作成されたコンテンツファイルを入力する。また、３４はコンテンツ暗号化部であり、コンテンツ入力部３３より入力されたコンテンツファイルを、コンテナ鍵生成部３１により生成されたコンテナ鍵を用いて暗号化する。

【００６８】また、３５はコンテナ化部であり、上記コンテンツ暗号化部３４により暗号化されたコンテンツファイルに対し、図３の利用情報設定部６により設定された利用可能情報を付加することにより、暗号化コンテンツとそのコンテンツの利用に必要な利用可能情報とを１つのファイルにまとめたコンテナを生成する。３６はコンテナ出力部であり、上記コンテナ化部３５により生成されたコンテナを外部に出力する。このように生成されたコンテナは、例えば販売店を介してそのウェブサイト上から利用者端末３に無料でダウンロードされたり、あるいはＣＤ－ＲＯＭ等を用いて配付される。

【００６９】販売店端末２は、利用情報設定部８とコンテナエンコーダ９とを備える。これらの機能については第１の実施形態と同様なので、ここでは説明を省略する。利用者端末３は、コンテナデコーダ２０を備える。このコンテナデコーダ２０は、コンテンツ作成者や販売店から配付を受けたコンテナに対して所定の処理を行うことによってコンテナ内のコンテンツを利用できる形態にするものであり、例えば図５のように構成される。

【００７０】図５において、４１はコンテナ入力部であり、上記コンテンツ作成者や販売店から配付を受けたコンテナを入力する。４２は利用情報抽出部であり、コンテナ内に付加情報として埋め込まれている利用可能情報を抽出する。ユーザは、このコンテナ内から抽出した利用可能情報を参照して、どの用途でコンテンツを利用するかを決定する。このときユーザは、暗号化コンテンツの復号を行うのに必要なコンテナ鍵に加えて、利用するコンテンツの用途を表す利用許可情報をライセンス発行センタ２１から購入する。ユーザは、購入した利用許可情報の制限下でコンテンツを利用できることになる。

【００７１】４３はコンテンツ抽出部であり、コンテナ内に含まれている暗号化コンテンツを抽出する。４４はコンテンツ復号化部であり、コンテンツ抽出部４３によりコンテナ内から抽出された暗号化コンテンツを、上述のコンテナ鍵と後述するユーザ鍵とを用いて復号し、コンテンツを利用できる形態にする。４５は鍵入手部であり、コンテンツを利用するユーザからの要求に応じて、上記コンテナ鍵とユーザ鍵をライセンス発行センタ２１から入手する。

【００７２】その際にユーザは、課金センタ２２に対して用途に応じた利用料を支払うことが必要であり、例えばコンテナ鍵は、課金センタ２２からライセンス発行センタ２１に決済通知があったことを条件にライセンス発行センタ２１から発行される。一方、ユーザ鍵は、例えば、ユーザがコンテナデコーダ２０を入手する際に、ライセンス発行センタ２１に対してユーザ登録を行うことを条件にライセンス発行センタ２１から発行される。なお、ユーザ鍵も課金を条件として発行するようにしても良い。

【００７３】上記ライセンス発行センタ２１は、図３に示すように鍵管理部２３を備えている。この鍵管理部２３は、例えば図６のように構成される。図６において、５１はユーザ鍵生成部であり、代金を支払ったユーザだけにコンテンツの利用を可能とするために、利用者端末３内のコンテナデコーダ２０においてコンテナ内のコンテンツファイルを利用できる形にする際に必要なユーザ鍵を生成する。このユーザ鍵は、個々のユーザに固有の鍵であり、第三者への譲渡は不可能である。

【００７４】例えば、ユーザがライセンス発行センタ２１から利用者端末３にコンテナ鍵をダウンロードする際に、ライセンス発行センタ２１において、ユーザ鍵を用いてコンテナ鍵に所定の処理を行うことにより、ユーザ鍵がなければコンテナ鍵を使って暗号化コンテンツを復号できないようにする。このようにコンテナ鍵の他にユーザ鍵がないとコンテンツの利用ができないようにする処理のことを、以下では「ユーザ鍵でロックする」と言う。なお、このロックの例としては暗号化処理がある。

【００７５】５２はユーザ鍵管理部であり、ユーザからの要求に応じてユーザ登録を行い、ユーザ鍵生成部５１によりそれぞれのユーザ毎に生成されたユーザ鍵を管理する。５３はコンテナ鍵収集部であり、コンテンツ作成者端末１内のコンテナエンコーダ１９においてそれぞれのコンテンツ毎に生成されたコンテナ鍵を収集する。５４はコンテナ鍵管理部であり、上記コンテナ鍵収集部５３により収集されたコンテナ鍵を管理する。

【００７６】５５は鍵発行部であり、ユーザが選択した

利用用途に応じた料金の支払いが完了した旨の通知を課金センタ２２から受けて、そのユーザに対してコンテナ鍵を発行するとともに、その選択した用途にコンテンツの利用を制限する利用許可情報も発行する。ここで、コンテナ鍵については、上述したようにユーザ鍵でロックすることにより、そのユーザにしか使用できないコンテナ鍵に変換したしたものを発行する。この鍵発行部５５はまた、ユーザからのユーザ登録に応じてユーザ鍵も発行する。

【００７７】また、上記課金センタ２２は、図３に示すように課金部２４および料金分配部２５を備えている。課金部２４は、ユーザが利用可能情報の中から選択した利用方法に準じる代金を受け取る。そして、課金処理が済んだ後に、ライセンス発行センタ２１に決済完了を通知する。また、料金分配部２５は、受け取った代金をコンテンツの権利者および販売店に対して著作権料および販売手数料として分配する処理を行う。

【００７８】図７は、上記図３～図６のように構成したコンテンツ流通システムにおいて行われる一連の動作を説明するための図である。図７において、まず最初にコンテンツ作成者やプロダクション等の著作者は、コンテンツ作成者端末１にてコンテンツを作成する。また著作者は、コンテンツの利用可能範囲や著作権料を決めて利用可能情報を設定する。さらに著作者は、コンテナエンコーダ１９を用いてコンテンツと利用可能情報とをコンテナ化し、コンテナファイルを生成する。

【００７９】このコンテナ化の際に、コンテナエンコーダ１９は、暗号鍵であるコンテナ鍵を生成し、そのコンテナ鍵でコンテンツファイルを暗号化してコンテナに組み込む。さらにコンテナエンコーダ１９は、生成したコンテナ鍵をライセンス発行センタ２１に登録するとともに、著作者により設定された著作権料を課金センタ２２に登録する。また、著作者は、以上のようにして作成したコンテナファイルを販売店に納める。

【００８０】販売店は、自らの販売手数料を上乗せしてコンテナの販売価格（利用料）を設定し、コンテナエンコーダ９を用いてコンテナファイル内の利用可能情報に追加する。このときコンテナエンコーダ９は、設定された販売手数料を課金センタ２２に登録する。ここで課金センタ２２に登録された販売店の販売手数料と、上記コンテンツ作成者端末１のコンテナエンコーダ１９により課金センタ２２に登録された著作権料とによって、ユーザが支払った代金の分配情報が構成される。

【００８１】販売店は、コンテナエンコーダ９を用いて２次的にコンテナ化したファイルを販売店のウェブサイトに掲載したり、ＣＤ－ＲＯＭに納めることなどによってコンテナの販売を行う。ユーザは、販売店のウェブサイトからコンテナをダウンロードしたり、ＣＤ－ＲＯＭを介してコンテナを入手する。そして、入手したコンテナ内の利用可能情報を参照して利用可能な用途と利用価格を把握し、利用したい用途を選択する。

【００８２】そして、ユーザは、選択した用途に応じた利用料を課金センタ２２を通して支払う。これに応じて課金センタ２２は、課金処理の完了をライセンス発行センタ２１に通知する。この通知を受けたライセンス発行センタ２１は、支払い価格に準じた利用許可情報とコンテナ鍵（ユーザ鍵でロックされたもの）をユーザに対して発行する。これとは別に、ライセンス発行センタ２１はユーザからの要求に応じてユーザ鍵も発行する。

【００８３】このようにコンテナ鍵、ユーザ鍵および利用許可情報を入手することによって始めて、コンテナデコーダ２０が利用できるようになる。ユーザは、この利用可能となったコンテナデコーダ２０を用いて、コンテナ内のコンテンツを利用できる形態に変換する。このときコンテナデコーダ２０は、利用許可情報に記載された利用方法だけをユーザに許可する。これによりユーザは、自分が選択した方法でコンテンツを利用することができるようになる。

【００８４】さらに、課金センタ２２では、ユーザからコンテンツの利用料を徴収する。そして、コンテンツ作成者端末１より登録された著作権料と、販売店端末２より登録された販売手数料とから成る分配情報をもとに、ユーザから支払われたコンテンツの利用代金をコンテンツ権利者と販売店に分配する。このとき、コンテンツ権利者に対する著作権料は、図７のように著作権管理団体２６を通して支払われることもある。

【００８５】なお、図７に示すように、ユーザが利用可能情報の中から選択した用途情報等をもとに、ユーザ情報やコンテンツの利用状況を課金センタ２２において収集して、それをコンテンツ作成者やプロダクションに通知したり、マーケティング情報として販売店に提供したりするようにしても良い。

【００８６】以上説明したように、第２の実施形態では、各コンテナ毎に固有のコンテナ鍵の他に、各ユーザ毎に固有のユーザ鍵も用いてコンテンツの利用を制限するようにしている。これにより、コンテナ鍵に相当する暗号鍵しかなかった従来の超流通システムと異なり、コンテナ鍵を第三者に転売しても、そのコンテナ鍵のロックを解くためのユーザ鍵を持たない第三者はコンテンツを利用できないようにすることができ、コンテナ鍵を正当に購入したユーザだけにそのコンテンツの利用を確実に制限することができる。よって、コンテンツの不正利用をより有効に防止することができる。

【００８７】なお、上記実施形態では、ライセンス発行センタ２１からコンテナ鍵をユーザがダウンロードする際に、ライセンス発行センタ２１においてコンテナ鍵をユーザ鍵でロックする例を示したが、この形態に限定されるものではない。例えば、コンテナファイルをユーザがダウンロードする際に、コンテンツ作成者端末１または販売店端末２においてコンテナファイルをユーザ鍵で

ロックするようにしても良い。

【００８８】また、利用者端末３内のコンテナデコーダ２０において、ユーザがコンテンツファイルをダウンロードした際にそのコンテナファイルをユーザ鍵でロックするようにしても良い。さらに、利用者端末３内のコンテナデコーダ２０において、ユーザがコンテナ鍵をダウンロードした際にそのコンテナ鍵をユーザ鍵でロックするようにしても良い。

【００８９】また、上記実施形態では、ユーザが入手したコンテナ内から利用可能情報を抽出し、これを参照して利用可能な用途を選択する例を示したが、この形態に限定されるものではない。例えば、ライセンス発行センタ２１がコンテンツ権利者や販売店から利用可能情報を収集し、ユーザからの要求に応じてその利用可能情報を提供するようにしても良い。

【００９０】（第３の実施形態）次に、本発明によるコンテンツ流通システムの第３の実施形態について説明する。以下に述べる第３の実施形態は、第１の実施形態に示した電子透かしと第２の実施形態に示した超流通システムとを組み合わせたものである。

【００９１】上記第２の実施形態によれば、正当にコンテナ鍵を購入したユーザだけがそのコンテンツを利用することが可能となる仕組みを提供できるが、抜き出し利用されたコンテンツのその後の不正利用については特に考慮していない。第３の実施形態は、この抜き出し利用されたコンテンツのその後の不正利用も有効に摘発できるようにしたものである。

【００９２】図８は、第３の実施形態によるコンテンツ流通システムの全体構成を示すブロック図である。なお、図８において、図１および図３に示した符号と同一の符号を付したものは、同一の機能を有するものであるので、これについての詳細な説明は省略する。

【００９３】図８に示すように、第３の実施形態に係るコンテンツ流通システムは、コンテンツ作成者端末１、販売店端末２、利用者端末３、不正流出監視センタ４、ライセンス発行センタ２１および課金センタ２２が、インターネットやＣＤ－ＲＯＭ等の情報伝達媒体５を介して以下に述べるような種々の情報をやり取りすることができるように構成されている。

【００９４】なお、ここでは図面の都合上、コンテンツ作成者端末１、販売店端末２、利用者端末３を１つずつ示しているが、それぞれ複数存在しても良い。また、不正流出監視センタ４、ライセンス発行センタ２１および課金センタ２２の構成は、それぞれ図１および図３に示したものと同様である。

【００９５】本実施形態のコンテンツ作成者端末１は、利用情報設定部１８とコンテナエンコーダ１９とを備える。利用情報設定部１８は、図１や図３に示した利用情報設定部６と同様に制限情報、価格情報、用途情報などから成る利用可能情報を設定する機能を持つが、設定可能な用途の範囲が広い点で上述の実施形態と異なる。すなわち、第１、第２の実施形態では、コンテンツの用途としては再生利用、もしくはウェブページへの張り付け利用の何れかであったが、本実施形態では以下に述べるような多種の用途を設定可能である。

【００９６】すなわち、コンテンツが静止画や動画の場合、用途情報としては、コンテンツの表示、コピー、編集、印刷、ウェブページへの張り付け、コピーしたコンテンツの配付などの情報を含む。また、コンテンツが音楽の場合は、コンテンツの再生、コピー、編集、デジタル録音、ウェブページへの張り付け、コピーしたコンテンツの配付などの情報を含む。

【００９７】図９は、上記図８のように構成したコンテンツ流通システムにおいて行われる一連の動作を説明するための図である。図９において、まず最初にコンテンツ作成者やプロダクション等の著作者は、コンテンツ作成者端末１においてコンテンツを作成し、その作成したコンテンツを不正流出監視センタ４に預ける。不正流出監視センタ４は、電子透かしエンコーダ１３を用いて、預かったコンテンツ内にコンテンツＩＤを電子透かしとして埋め込み、それをコンテンツ作成者端末１に返す。

【００９８】また、著作者は、コンテンツの利用可能範囲や著作権料を決めて、利用可能情報を設定する。このとき、コンテンツ作成者端末１内のコンテナエンコーダ１９によって、利用可能情報でウェブページへの掲載が許可されたコンテンツのＩＤが不正流出監視センタ４に通知され、利用許可ＤＢ１２に登録される。さらに著作者は、コンテナエンコーダ１９を用いて、電子透かしの埋め込まれたコンテンツと利用可能情報とをコンテナ化し、コンテナファイルを生成する。

【００９９】このコンテナ化の際に、コンテナエンコーダ１９は、暗号鍵であるコンテナ鍵を生成し、そのコンテナ鍵でコンテンツファイルを暗号化してコンテナに組み込む。さらにコンテナエンコーダ１９は、生成したコンテナ鍵をライセンス発行センタ２１に登録するとともに、著作者により設定された著作権料を課金センタ２２に登録する。また、著作者は、以上のようにして作成したコンテナファイルを販売店に納める。

【０１００】販売店は、自らの販売手数料を上乗せしてコンテナの販売価格（利用料）を設定し、コンテナエンコーダ９を用いてコンテナファイル内の利用可能情報に追加する。このときコンテナエンコーダ９は、設定された販売手数料を課金センタ２２に登録する。ここで課金センタ２２に登録された販売店の販売手数料と、上記コンテンツ作成者端末１のコンテナエンコーダ１９により課金センタ２２に登録された著作権料とによって、ユーザが支払った代金の分配情報が構成される。

【０１０１】販売店は、コンテナエンコーダ９を用いて２次的にコンテナ化したファイルを販売店のウェブサイトに掲載したり、ＣＤ－ＲＯＭに納めることなどによっ

てコンテナの販売を行う。なお、著作者自身が販売店となってコンテナを販売することも可能である。

【０１０２】ユーザは、販売店のウェブサイトからコンテナをダウンロードしたり、ＣＤ－ＲＯＭを介してコンテナを入手する。そして、入手したコンテナ内の利用可能情報を参照して利用可能な用途と利用価格を把握し、利用したい用途を選択する。このとき、コンテンツをウェブページに張り付けて利用することを選択した場合は、そのウェブページのＵＲＬとコンテンツＩＤとが利用ＵＲＬ登録部１１によってライセンス発行センタ２１に通知される。

【０１０３】ライセンス発行センタ２１は、その受け取ったＵＲＬとコンテンツＩＤとを更に不正流出監視センタ４に通知し、利用許可ＤＢ１２に登録する。なお、ここではＵＲＬとコンテンツＩＤの利用許可ＤＢ１２への登録をライセンス発行センタ２１を介して行っているが、第１の実施形態と同様に、利用者端末３から不正流出監視センタ４に直接行っても良い。

【０１０４】コンテンツの用途を選択したユーザは、その選択した用途に応じた利用料を課金センタ２２を通して支払う。これに応じて課金センタ２２は、課金処理の完了をライセンス発行センタ２１に通知する。この通知を受けたライセンス発行センタ２１は、支払い価格に準じた利用許可情報とコンテナ鍵（例えば、ユーザ鍵でロックされたもの）をユーザに対して発行する。これとは別に、ライセンス発行センタ２１はユーザからの要求に応じてユーザ鍵も発行する。

【０１０５】このようにコンテナ鍵、ユーザ鍵および利用許可情報を入手することによって始めて、コンテナデコーダ２０が利用できるようになる。ユーザは、この利用可能となったコンテナデコーダ２０を用いて、コンテナ内のコンテンツを利用できる形態に変換する。このときコンテナデコーダ２０は、利用許可情報に記載された利用方法だけをユーザに許可する。これによりユーザは、自分が選択した方法でコンテンツを利用することができるようになる。

【０１０６】ここで、ユーザが再生利用を選択していた場合、コンテナデコーダ２０は、コンテナ鍵を用いてコンテナファイル内の暗号化コンテンツを内部メモリ上で復号し、静止画や動画であれば表示あるいは印刷する。また、音楽であればスピーカに出力する。ただし、汎用の画像フォーマットや音楽フォーマットのファイルとして外部記憶装置に書き込むことはしない。よって、再生後にユーザの手元にコンテンツファイルが残ることはなく、ユーザは復号データのコピー、編集、ウェブページへの張り付けなどは行うことができず、またコピーしたコンテンツを他者に勝手に配付することもできない。つまり、この場合ユーザは、コンテンツを個人的用途のために再生することだけが可能である。

【０１０７】一方、コピー、編集、ウェブページへの張り付けなどの抜き出し許可をユーザが選択していた場合、コンテナデコーダ２０は、内部メモリ上で復号したコンテンツファイルを汎用フォーマットのデータファイルに変換してコンテナデコーダ２０の外部に出力し、外部記憶装置に書き込む。これにより、ユーザは、汎用フォーマットのコンテンツファイルをユーザ所有のウェブページに張り付けることなどが可能となる。

【０１０８】不正流出監視センタ４では、コンテンツ探索部１４（エージェントで構成される検索ロボット）を用いて、インターネット上のウェブサイトを巡回して各ウェブページに置かれたコンテンツを順次ダウンロードする。このとき、不正流出しているコンテンツがウェブページ上に置かれていれば、それもダウンロードされる。

【０１０９】さらに、不正流出監視センタ４では、電子透かしデコーダ１５を用いて、ダウンロードしたコンテンツの中から電子透かしを取り出し、そのコンテンツに固有のＩＤを検出する。そして、不正検出部１６において、その検出したコンテンツＩＤおよびダウンロード先のＵＲＬと、利用許可ＤＢ１２に登録されているコンテンツＩＤおよびＵＲＬとを照合することにより、コンテンツの不正利用の検出を行う。

【０１１０】すなわち、利用許可ＤＢ１２に登録されていないコンテンツＩＤを検出した場合や、ユーザが正規料金を支払ってコンテンツを張り付けたウェブページのＵＲＬ以外の場所でコンテンツＩＤを検出した場合には、そのコンテンツは無許可で張り付けられたものということになる。よって、この場合には、不正通知部１７を用いて、不正利用を摘発したコンテンツＩＤとそれが置かれていたウェブページのＵＲＬとをそのコンテンツの著作者に通知する。また、そのウェブページの運営者に警告を発するようにしても良い。

【０１１１】さらに、課金センタ２２では、ユーザからコンテンツの利用料を徴収する。そして、コンテンツ作成者端末１より登録された著作権料と、販売店端末２より登録された販売手数料とから成る分配情報をもとに、ユーザから支払われたコンテンツの利用代金をコンテンツ権利者と販売店に分配する。このとき、コンテンツ権利者に対する著作権料は、図９のように著作権管理団体２６を通して支払われることもある。

【０１１２】以上説明したように、第３の実施形態では、ユーザがコンテンツを利用可能とするための鍵としてコンテナ鍵とユーザ鍵とを用いているので、コンテナ鍵を正当に購入したユーザだけにそのコンテンツの利用を制限することができる。しかも、本実施形態では、コンテンツに埋め込んだ電子透かしを利用してウェブページへの不正流出も監視しているので、コンテナ鍵を正当に購入したユーザによって汎用フォーマットに変換されたコンテンツが無断で第三者に配付され、第三者のウェブページ上でそのコンテンツの販売が行われるなどの不

正利用も確実に発見することができる。

【０１１３】入手したコンテンツをコピーして転売したり、あるいは適当に編集して販売するなどの不正利用は、コンテンツをウェブページ上に掲載することによって行われるケースが多いため、コンテンツのウェブページへの不正流出を摘発することによって、コンテンツの著作権保護を格段に向上させることができる。これにより、従来超流通システムにおいて不正流出の観点から課せられていた利用制限から開放され、様々な用途にコンテンツを利用することができる。

【０１１４】なお、上記第３の実施形態では、コンテンツファイルをコンテナ化する前に不正流出監視センタ４において電子透かしを埋め込む例を示しているが、電子透かしは、最終的にユーザが入手したコンテンツをウェブページに張り付けるまでの間に埋め込まれていれば良く、その埋め込む場所やタイミングは上記の例に限定されない。例えば、ユーザが利用者端末３上に入手したコンテナからコンテンツを取り出すときに電子透かしを埋め込むようにしても良い。

【０１１５】また、上記実施形態では、コンテンツ作成者端末１と利用者端末３の両方から不正流出監視センタ４の利用許可ＤＢ１２にウェブページ張り付けの利用許可に関する情報を登録しているが、どちらか一方のみから登録を行うようにしても良い。また、ここでは利用許可に関する情報を登録しているが、利用拒否に関する情報を登録するようにしても良い。

【０１１６】また、上記実施形態では、コンテンツを利用可能情報と共に１つのファイルにまとめたコンテナとして流通する例を示したが、必ずしもコンテナ化する必要はない。例えば、コンテンツの流通と利用可能情報の流通とを別個に行うようにしても良い。

【０１１７】また、上記実施形態では、ライセンス発行センタ２１からコンテナ鍵をユーザがダウンロードする際に、ライセンス発行センタ２１においてコンテナ鍵をユーザ鍵でロックする例を示したが、この形態に限定されるものではない。例えば、コンテナファイルをユーザがダウンロードする際に、コンテンツ作成者端末１または販売店端末２においてコンテナファイルをユーザ鍵でロックするようにしても良い。

【０１１８】また、利用者端末３内のコンテナデコーダ２０において、ユーザがコンテンツファイルをダウンロードした際にそのコンテナファイルをユーザ鍵でロックするようにしても良い。さらに、利用者端末３内のコンテナデコーダ２０において、ユーザがコンテナ鍵をダウンロードした際にそのコンテナ鍵をユーザ鍵でロックするようにしても良い。

【０１１９】また、上記実施形態では、ユーザが入手したコンテナ内から利用可能情報を抽出し、これを参照して利用可能な用途を選択する例を示したが、この形態に限定されるものではない。例えば、ライセンス発行センタ２１がコンテンツ権利者や販売店から利用可能情報を収集し、ユーザからの要求に応じてその利用可能情報を提供するようにしても良い。

【０１２０】（本発明の他の実施形態）なお、以上に説明した本実施形態のコンテンツ流通システムは、それぞれの端末やセンタが備えるコンピュータのＣＰＵあるいはＭＰＵ、ＲＡＭ、ＲＯＭなどで構成されるものであり、ＲＡＭやＲＯＭに記憶されたプログラムが動作することによって実現できる。

【０１２１】したがって、コンピュータが上記の機能を果たすように動作させるプログラムを例えばＣＤ－ＲＯＭのような記録媒体に記録し、これをコンピュータに読み込ませることによって実現できるものである。上記プログラムを記録する記録媒体としては、ＣＤ－ＲＯＭ以外に、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＤＶＤ、磁気テープ、不揮発性メモリカード等を用いることができる。

【０１２２】また、コンピュータが供給されたプログラムを実行することにより上述の実施形態の機能が実現されるだけでなく、そのプログラムがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部がコンピュータの機能拡張ボードや機能拡張ユニットにより行われて上述の実施形態の機能が実現される場合も、かかるプログラムは本発明の実施形態に含まれる。

【０１２３】なお、上記に説明した各実施形態は、何れも本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０１２４】

【発明の効果】本発明は上述したように、ネットワーク上のウェブページを探索してウェブページ上のコンテンツを順次取り込み、それらのコンテンツに電子透かしとして埋め込まれたコンテンツ識別情報と、ウェブページへの掲載の許否に関する管理情報とを照合しでデジタルコンテンツの不正利用を検出するようにしたので、ウェブページへの掲載が許可されていないコンテンツの不正利用等を電子透かしを用いて常に監視し、ネットワーク上で流通するデジタルコンテンツの著作権保護を図る仕組みを提供することができる。

【０１２５】また、本発明の他の特徴によれば、デジタルコンテンツの掲載が許可されたウェブページを表すリソース情報をコンテンツ識別情報と対応付けて管理し、このリソース情報も加味して不正検出を行うようにしたので、ウェブページへの掲載自体は許可されているが、許可されていないウェブページに掲載されたコンテンツ

の不正利用等を発見することができ、ネットワーク上で流通するデジタルコンテンツの著作権保護をより確実なものとすることができる。

【０１２６】また、本発明のその他の特徴によれば、デジタルコンテンツを暗号化する各コンテンツ毎に固有の暗号鍵の他に、デジタルコンテンツを利用する各ユーザ毎に固有のユーザ鍵も用いてデジタルコンテンツの利用を制限するようにしたので、デジタルコンテンツを正当に購入していない第三者にデジタルコンテンツとその暗号鍵を配付したとしても、ユーザ鍵を持たない第三者はそのデジタルコンテンツを利用できないようにすることができ、正当に購入したユーザだけにデジタルコンテンツの利用を制限することができる。よって、ネットワーク上で流通するデジタルコンテンツの著作権保護を更に確実なものとすることができる。

【０１２７】また、本発明のその他の特徴によれば、上述の電子透かしに関する発明とユーザ鍵に関する発明とを組み合わせて適用したので、正当に購入したユーザだけにデジタルコンテンツの利用を制限することができるだけでなく、正当にデジタルコンテンツを購入したユーザがその後、許可されていないにも関わらずウェブページへの掲載を行ったり、許可されていないウェブページへの掲載を行ったりすることなどの不正利用も確実に発見することができる。このように、本発明では、デジタルコンテンツを正当に購入した後の不正利用についてもケアしているので、デジタルコンテンツの利用方法の制限を緩和し、ユーザの要求に応じた様々な態様でデジタルコンテンツを提供することもできるようになる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態によるコンテンツ流通システムの全体構成を示すブロック図である。

【図２】図１のように構成したコンテンツ流通システムにおいて行われる一連の動作を説明するための図である。

【図３】本発明の第２の実施形態によるコンテンツ流通システムの全体構成を示すブロック図である。

【図４】第２の実施形態によるコンテンツ作成者端末が備えるコンテナエンコーダの構成例を示す図である。

【図５】第２の実施形態による利用者端末が備えるコンテナデコーダの構成例を示す図である。

【図６】第２の実施形態によるライセンス発行センタが備える鍵管理部の構成例を示す図である。

【図７】図３のように構成したコンテンツ流通システムにおいて行われる一連の動作を説明するための図である。

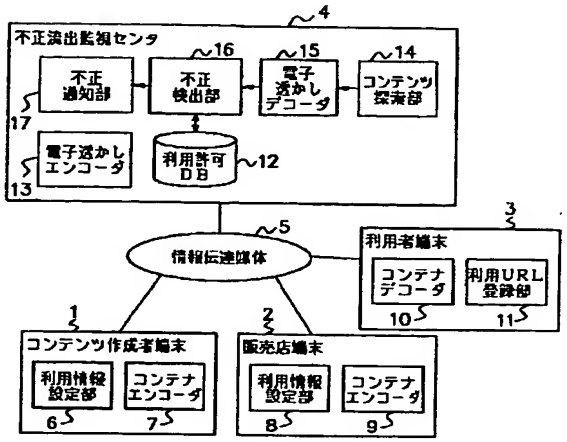
【図８】本発明の第３の実施形態によるコンテンツ流通システムの全体構成を示すブロック図である。

【図９】図８のように構成したコンテンツ流通システムにおいて行われる一連の動作を説明するための図である。

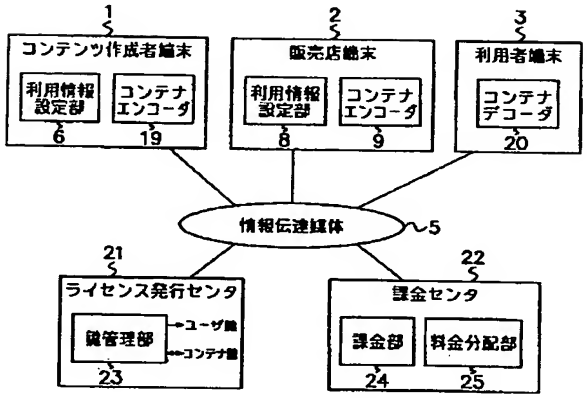
【符号の説明】

１　コンテンツ作成者端末
２　販売店端末
３　利用者端末
４　不正流出監視センタ
５　情報伝達媒体
６　利用情報設定部
７　コンテナエンコーダ
８　利用情報設定部
９　コンテナエンコーダ
１０　コンテナデコーダ
１１　利用ＵＲＬ登録部
１２　利用許可ＤＢ
１３　電子透かしエンコーダ
１４　コンテンツ探索部
１５　電子透かしデコーダ
１６　不正検出部
１７　不正通知部
１８　利用情報設定部
１９　コンテナエンコーダ
２０　コンテナデコーダ
２１　ライセンス発行センタ
２２　課金センタ
２３　鍵管理部
２４　課金部
２５　料金分配部
３１　コンテナ鍵生成部
３２　コンテナ鍵登録部
３３　コンテンツ入力部
３４　コンテンツ暗号化部
３５　コンテナ化部
３６　コンテナ出力部
４１　コンテナ入力部
４２　利用情報抽出部
４３　コンテンツ抽出部
４４　コンテンツ復号化部
４５　鍵入手部
５１　ユーザ鍵生成部
５２　ユーザ鍵管理部
５３　コンテナ鍵収集部
５４　コンテナ鍵管理部
５５　鍵発行部

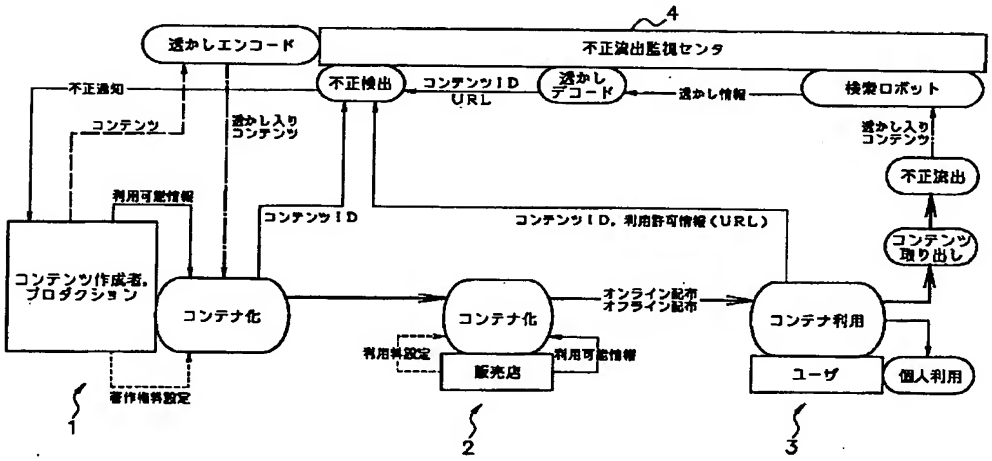
【図１】


不正流出監視センタ
不正通知部
不正検出部
電子透かしデコーダ
コンテンツ探索部
電子透かしエンコーダ
利用許可DB
情報伝達媒体
利用者端末
コンテナデコーダ
利用URL登録部
コンテンツ作成者端末
利用情報設定部
コンテナエンコーダ
販売店端末
利用情報設定部
コンテナエンコーダ

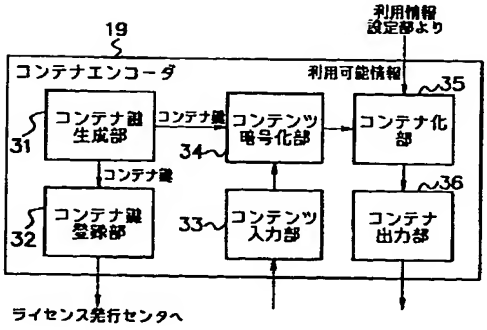
【図３】


コンテンツ作成者端末
利用情報設定部
コンテナエンコーダ
販売店端末
利用情報設定部
コンテナエンコーダ
利用者端末
コンテナデコーダ
情報伝達媒体
ライセンス発行センタ
鍵管理部
ユーザ鍵
コンテナ鍵
課金センタ
課金部
料金分配部

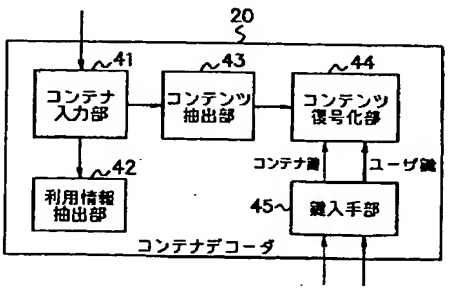
【図２】


透かしエンコード
不正流出監視センタ
不正通知
不正検出
コンテンツID URL
透かしデコード
透かし情報
検索ロボット
コンテンツ
透かし入りコンテンツ
利用可能情報
コンテンツID
コンテンツID，利用許可情報（URL）
不正流出
コンテンツ取り出し
コンテンツ作成者，プロダクション
コンテナ化
コンテナ化
オンライン配布
オフライン配布
コンテナ利用
利用料設定
販売店
利用可能情報
ユーザ
個人利用
著作権料設定

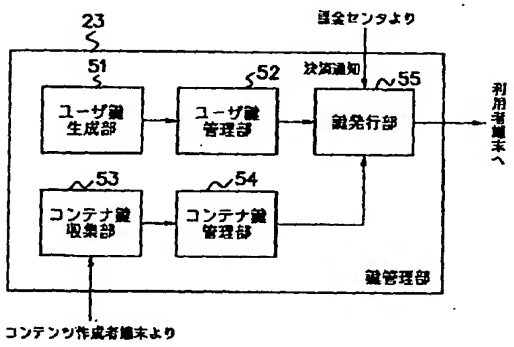
【図４】


利用情報設定部より
コンテナエンコーダ
利用可能情報
コンテナ鍵生成部
コンテナ鍵
コンテンツ暗号化部
コンテナ化部
コンテナ鍵
コンテナ鍵登録部
コンテンツ入力部
コンテナ出力部
ライセンス発行センタへ

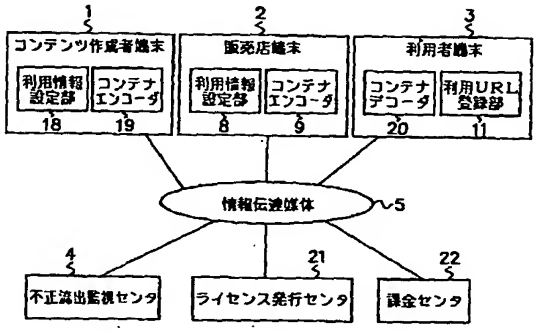
【図５】


コンテナ入力部
コンテンツ抽出部
コンテンツ復号化部
利用情報抽出部
コンテナ鍵
ユーザ鍵
鍵入手部
コンテナデコーダ

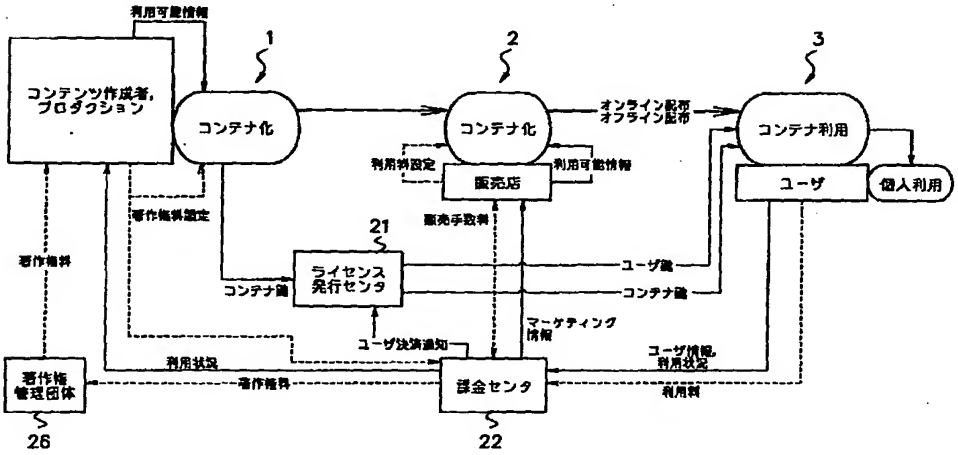
【図６】


23
課金センタより
51
52
決済通知
55
ユーザ鍵生成部
ユーザ鍵管理部
鍵発行部
利用者端末へ
53
54
コンテナ鍵収集部
コンテナ鍵管理部
鍵管理部
コンテンツ作成者端末より

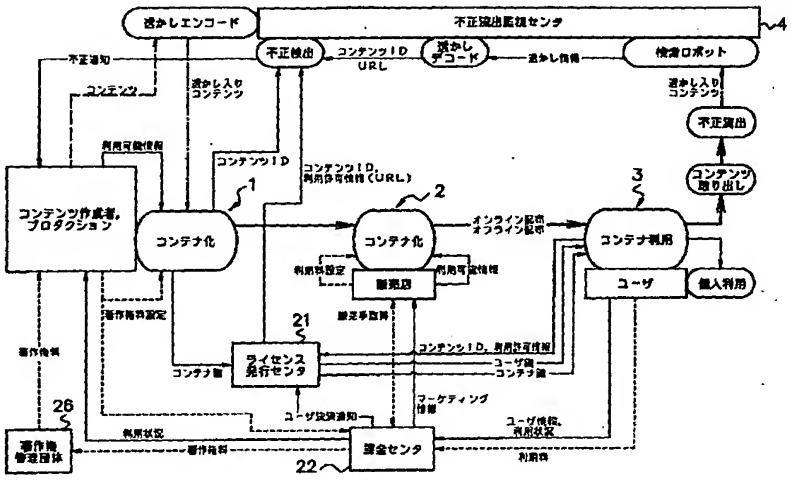
【図８】


1
2
3
コンテンツ作成者端末
販売店端末
利用者端末
利用情報設定部
コンテナエンコーダ
利用情報設定部
コンテナエンコーダ
コンテナデコーダ
利用URL登録部
18
19
8
9
20
11
情報伝達媒体
5
4
21
22
不正流出監視センタ
ライセンス発行センタ
課金センタ

【図７】


利用可能情報
1
2
3
コンテンツ作成者，プロダクション
コンテナ化
コンテナ化
オンライン配布
オフライン配布
コンテナ利用
利用料設定
販売店
利用可能情報
ユーザ
個人利用
著作権料設定
販売手数料
21
著作権料
ライセンス発行センタ
ユーザ鍵
コンテナ鍵
コンテナ鍵
マーケティング情報
ユーザ決済通知
利用状況
ユーザ情報，利用状況
著作権管理団体
著作権料
課金センタ
利用料
26
22

【図９】


透かしエンコード
不正検出監視センタ
4
不正検出
コンテンツID
URL
透かしデコード
検索ロボット
不正通知
コンテンツ
透かし入りコンテンツ
透かし情報
不正資出
コンテンツ取り出し
利用可能情報
コンテンツID
コンテンツID、利用許可情報（URL）
1
2
3
コンテンツ作成者、プロダクション
コンテナ化
コンテナ化
コンテナ利用
オンライン配信
オフライン配信
利用状態設定
販売店
利用可能情報
ユーザ
個人利用
著作権情報設定
販売手数料
21
著作権情
ライセンス発行センタ
コンテンツID、利用許可情報
コンテナ鍵
ユーザ鍵
コンテナ鍵
マーケティング情報
26
ユーザ登録通知
ユーザ情報、利用状況
著作権管理団体
利用状況
著作権料
課金センタ
22
利用料